FIG. 1

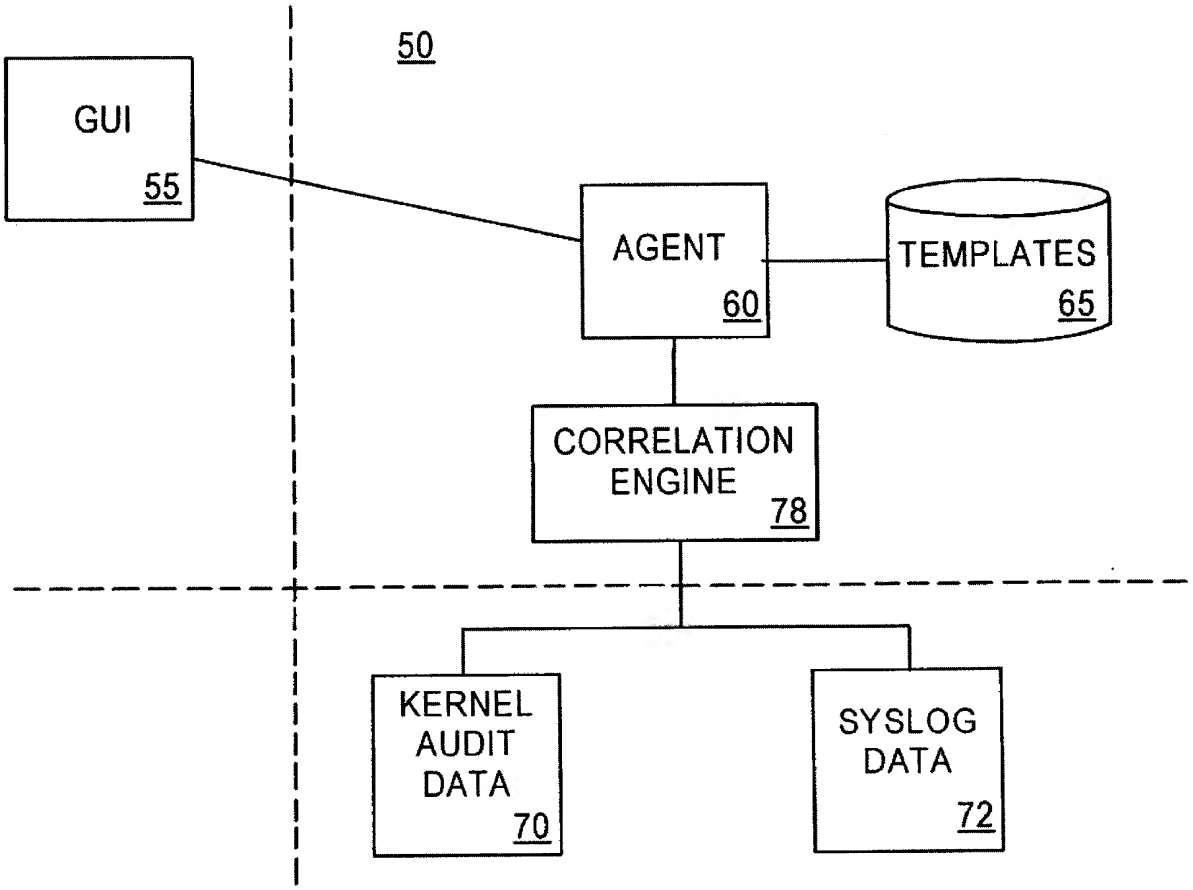

50
GUI
55
AGENT
60
TEMPLATES
65
CORRELATION ENGINE
78
KERNEL AUDIT DATA
70
SYSLOG DATA
72

FIG. 2

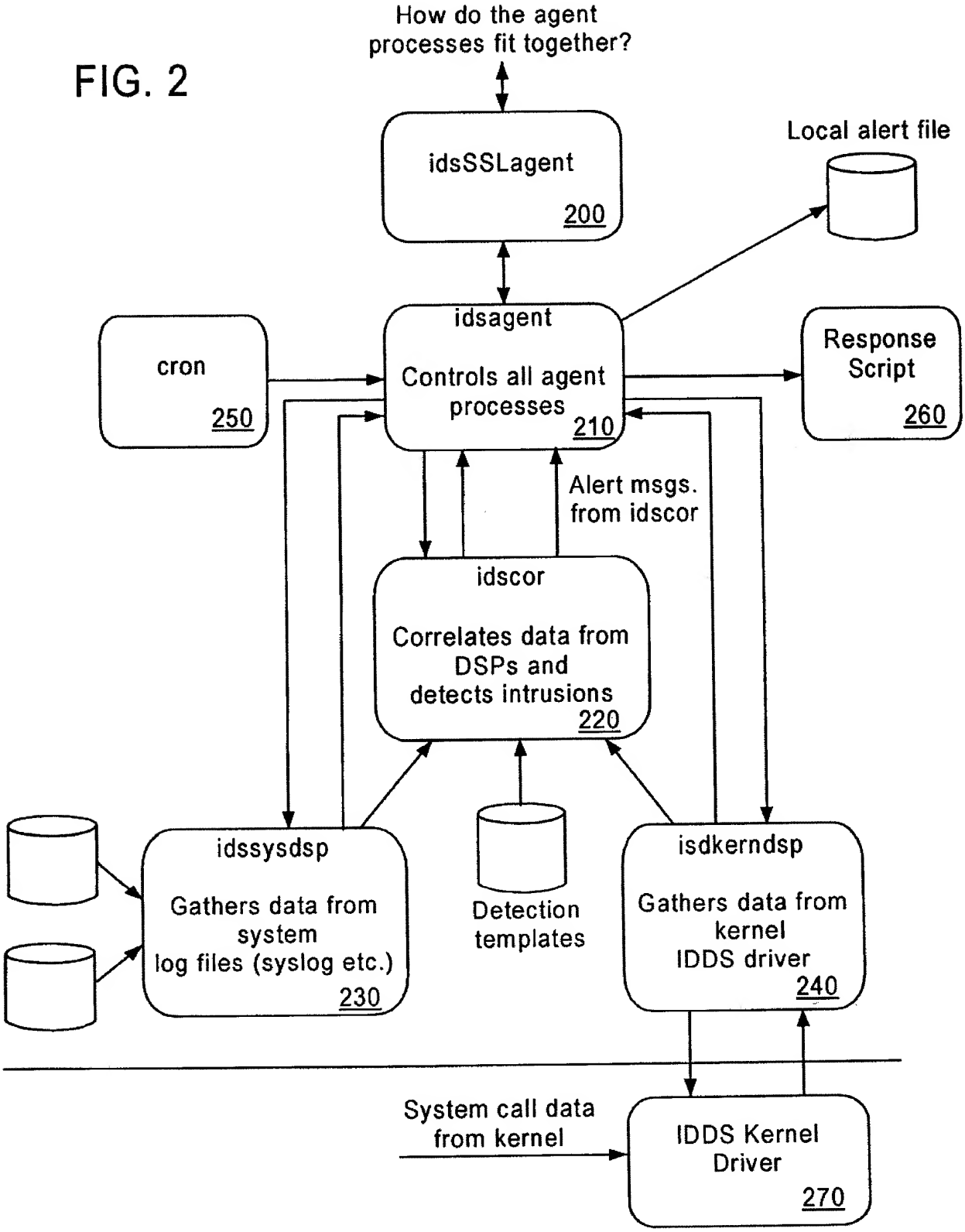

How do the agent processes fit together?
idsSSLagent
200
Local alert file
idsagent
Controls all agent processes
210
cron
250
Response Script
260
Alert msgs. from idscor
idscor
Correlates data from DSPs and detects intrusions
220
idssysdsp
Gathers data from system log files (syslog etc.)
230
Detection templates
isdkerndsp
Gathers data from kernel IDDS driver
240
System call data from kernel
IDDS Kernel Driver
270

FIG. 3

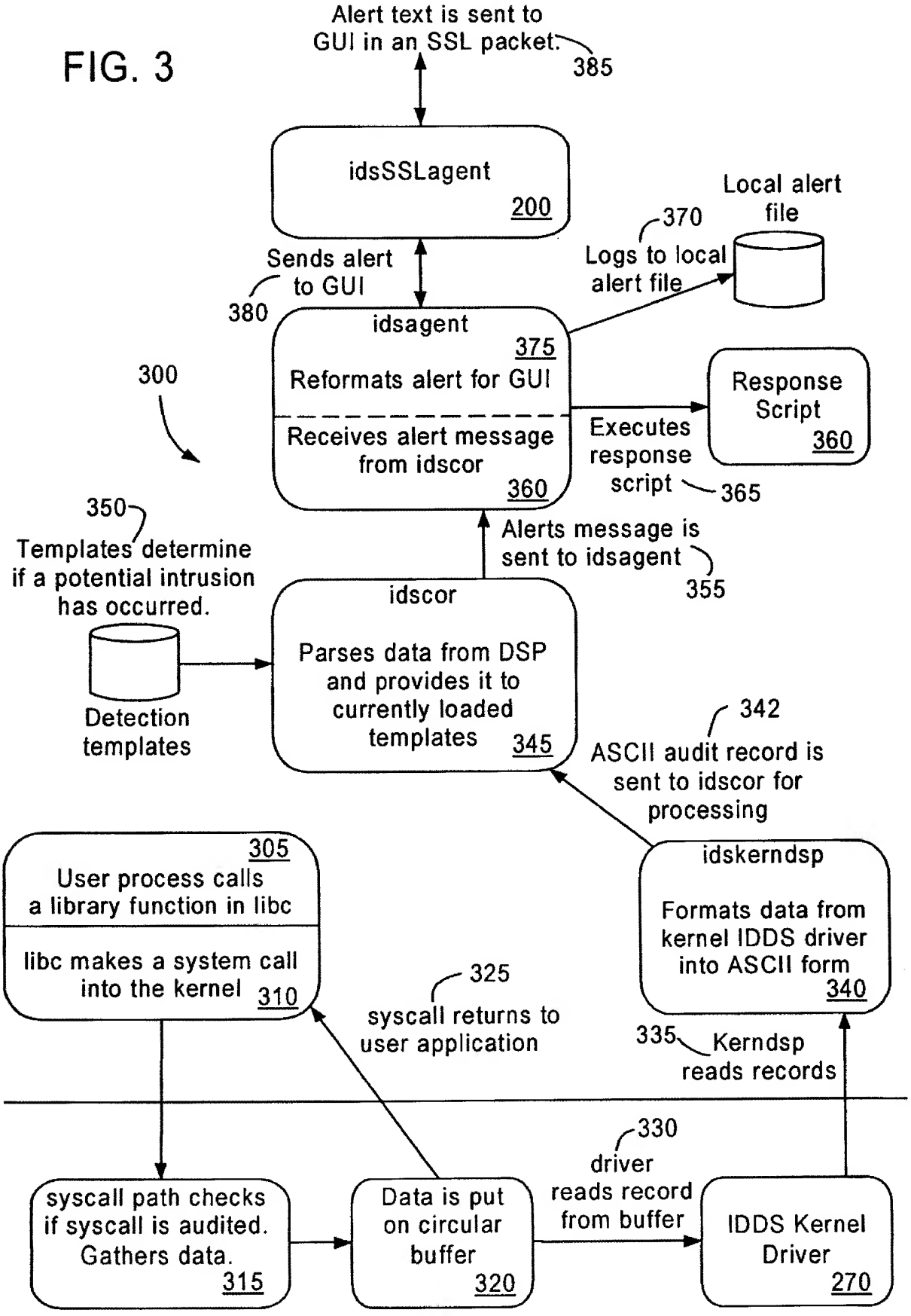

Alert text is sent to GUI in an SSL packet.
385
idsSSLagent
200
Local alert file
370
Logs to local alert file
Sends alert to GUI
380
idsagent
375
Reformats alert for GUI
Receives alert message from idscor
360
300
Response Script
360
Executes response script
365
350
Templates determine if a potential intrusion has occurred.
Alerts message is sent to idsagent
355
idscor
Parses data from DSP and provides it to currently loaded templates
345
Detection templates
342
ASCII audit record is sent to idscor for processing
idskerndsp
Formats data from kernel IDDS driver into ASCII form
340
305
User process calls a library function in libc
libc makes a system call into the kernel
310
325
syscall returns to user application
335
Kerndsp reads records
330
driver reads record from buffer
syscall path checks if syscall is audited. Gathers data.
315
Data is put on circular buffer
320
IDDS Kernel Driver
270

FIG. 4

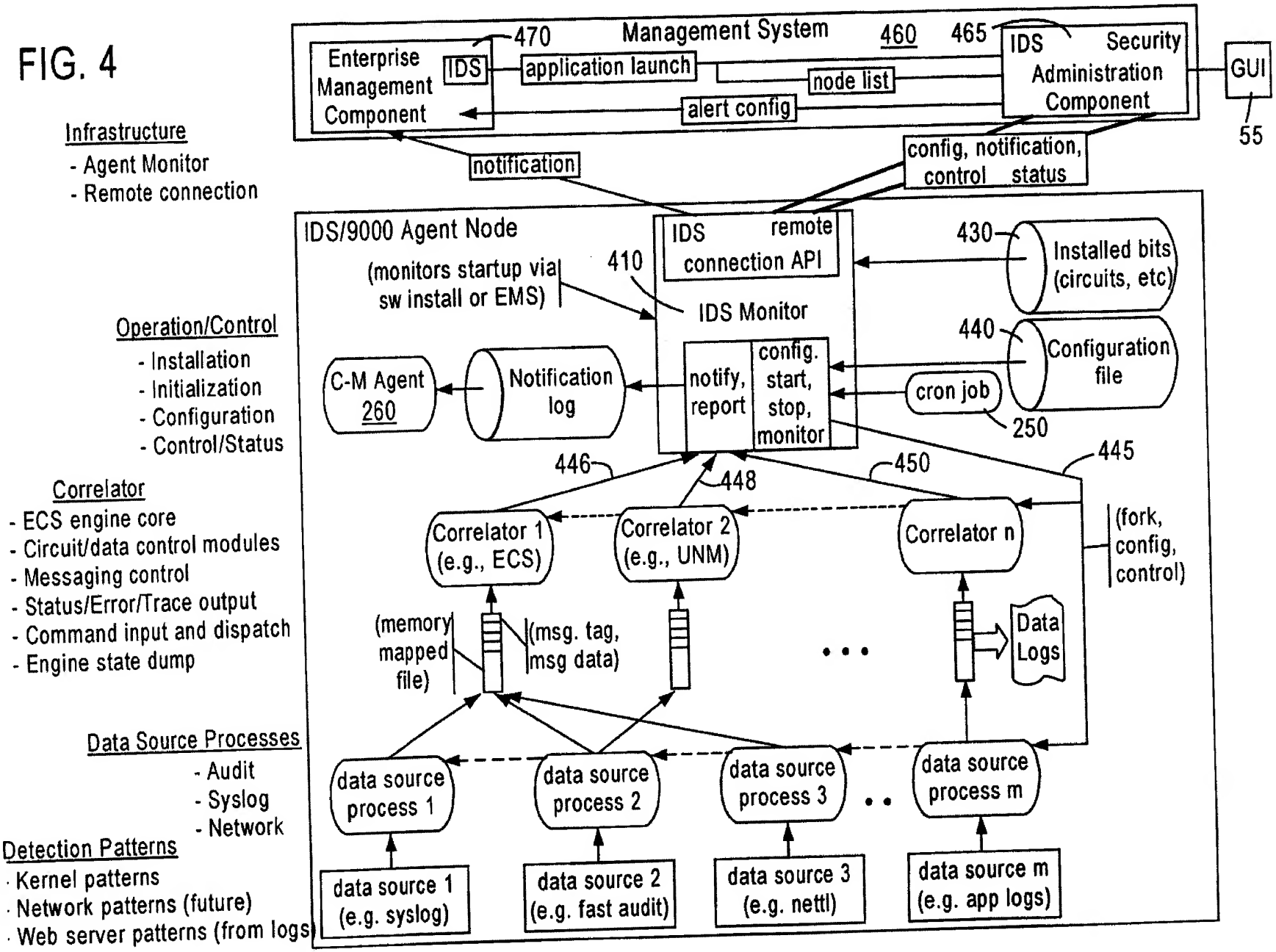
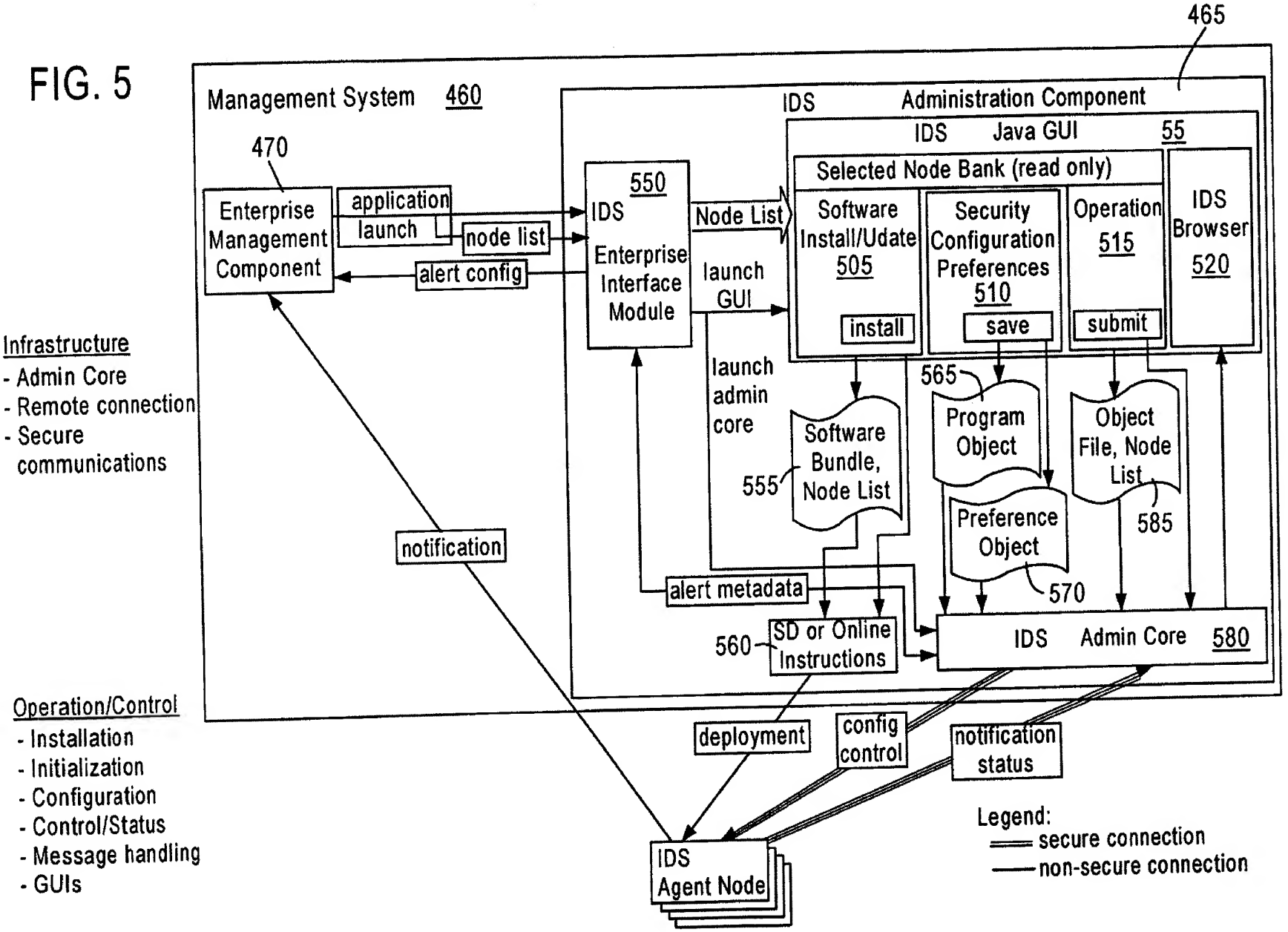

Infrastructure
- Agent Monitor
- Remote connection
Operation/Control
- Installation
- Initialization
- Configuration
- Control/Status
Correlator
- ECS engine core
- Circuit/data control modules
- Messaging control
- Status/Error/Trace output
- Command input and dispatch
- Engine state dump
Data Source Processes
- Audit
- Syslog
- Network
Detection Patterns
- Kernel patterns
- Network patterns (future)
- Web server patterns (from logs)
Management System
460
470
Enterprise Management Component
IDS
application launch
node list
alert config
465
IDS Security Administration Component
GUI
55
notification
config, notification, control status
IDS/9000 Agent Node
IDS remote connection API
410
IDS Monitor
(monitors startup via sw install or EMS)
430
Installed bits (circuits, etc)
440
Configuration file
cron job
250
notify, report
config. start, stop, monitor
C-M Agent 260
Notification log
446
448
450
445
Correlator 1 (e.g., ECS)
Correlator 2 (e.g., UNM)
Correlator n
(fork, config, control)
(memory mapped file)
(msg. tag, msg data)
Data Logs
data source process 1
data source process 2
data source process 3
data source process m
data source 1 (e.g. syslog)
data source 2 (e.g. fast audit)
data source 3 (e.g. nettl)
data source m (e.g. app logs)

FIG. 5


Management System 460
465
IDS Administration Component
IDS Java GUI 55
470
Enterprise Management Component
application launch
node list
alert config
550
IDS Enterprise Interface Module
Node List
launch GUI
Selected Node Bank (read only)
Software Install/Udate 505
Security Configuration Preferences 510
Operation 515
IDS Browser 520
install
save
submit
launch admin core
565
Program Object
Object File, Node List
585
Software Bundle, Node List
555
Preference Object
570
notification
alert metadata
560
SD or Online Instructions
IDS Admin Core 580
deployment
config control
notification status
IDS Agent Node
Infrastructure
- Admin Core
- Remote connection
- Secure communications
Operation/Control
- Installation
- Initialization
- Configuration
- Control/Status
- Message handling
- GUIs
Legend:
secure connection
non-secure connection